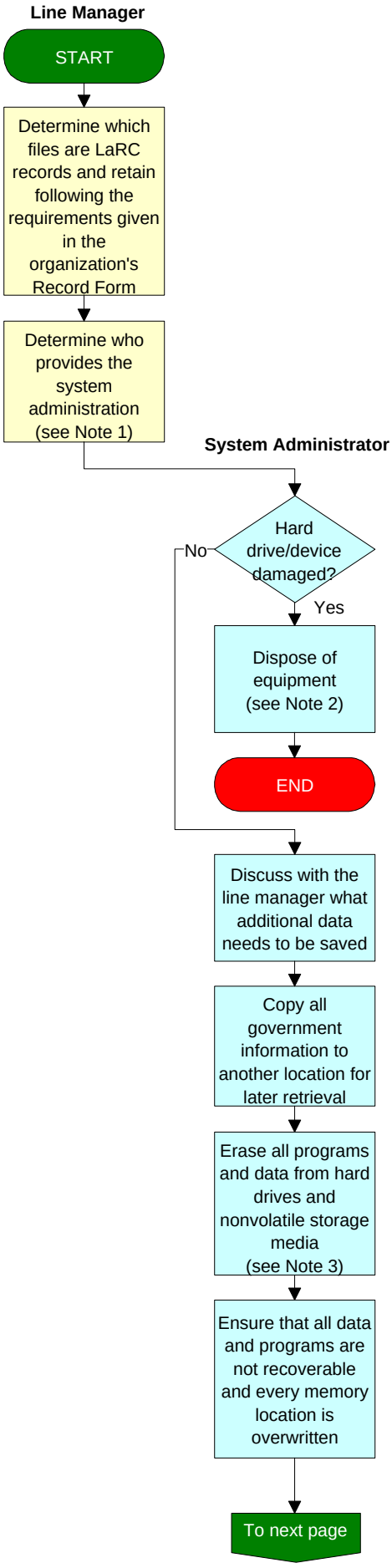
CLEANING AND EXCESS OF COMPUTER HARD DRIVES AND OTHER IT-RELATED NONVOLATILE STORAGE DEVICES

LMS-CP-5550
Revision: B-3

Objectives:
Prior to relocating, excessing, or repairing IT storage devices:
-Ensure Federal records are preserved appropriately
-Ensure the security of Federal information
-Avoid copyright violations
-Avoid the disclosure of sensitive and privacy information
-Ensure proper disposition of failed hard drives and other storage devices
-Ensure that hard drives are properly cleaned and that data is cleared from other nonvolatile storage devices

Approval Original signed on file
Associate Director for Research and Technology Competencies



General Information

No official records are generated by the implementation of this procedure.

Note 1
The Line Manager with responsibility for the system to which the storage device is connected is responsible for ensuring that the storage device is cleaned by the System Administrator assigned to the system. If the System Administrator is a Contractor, the Line Manager shall ensure that the tasks required to preserve Federal records and clean storage devices are defined in a task description or statement of work for the Contractor.

It is the responsibility of the System Administrator to physically clean the hard drive and to clear all nonvolatile storage devices; e.g., hand-held devices, external hard drives, routers, switchers, network servers, network printers, network facsimile devices, and mainframe computers. If the System Administrator has questions about the method and software needed to clean the drive, or if there is no assigned system administrator, check the web site http://itsecurity.larc.nasa.gov/ for information on software that is acceptable for cleaning hard drives or vendors with existing contracts to perform the cleaning of hard drives for Langley.

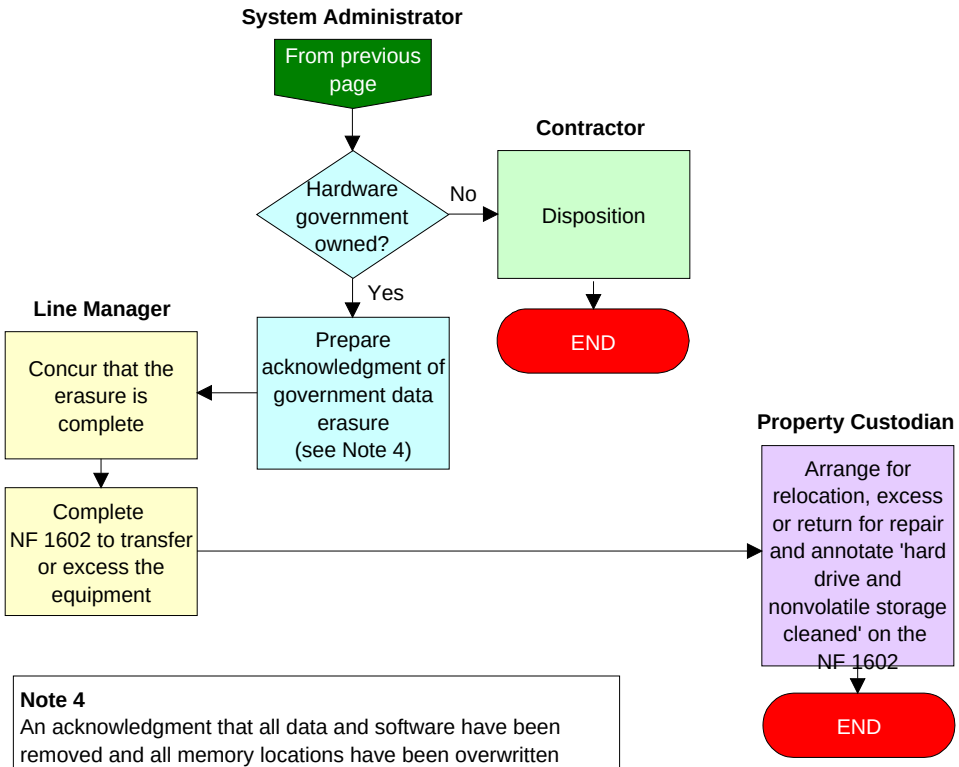
Note 2
Prepare NASA Form 1617, Request for Cannibalization/Modification of Controlled Equipment per NPR 4200.2, Equipment Management Manual for Property Custodians, paragraph 2.3, prior to removing the hard drive. For instructions on cannibalizing equipment see NPR 4200.2 and page 2 of NF 1617.

Send the storage device to Property Disposal for destruction. The LF 40 must indicate that the drive is damaged and must be destroyed. See LMS-CP-2722.

Considerations when damage prevents the hard drive from being erased:
-If the drive contains sensitive data such as export-controlled data/programs, proprietary information, restricted data or Privacy Act information, remove the drive and have it physically destroyed. This is true even if the drive is under warranty, since it is very likely that the information is more important or valuable than the cost of a new drive.
-If the failed device belongs to a contractor, the Line Manager must determine how the contractor proposes to dispose of the device. If the proposed disposal carries a risk of disclosure, then the Line Manager must procure the device and have it physically destroyed.

Note 3
If the information on the storage device is of high sensitivity or the cost of cleaning the device exceeds the cost of replacing the device, the line manager has the option of replacing the old device with a new comparable device and destroying the old device.

Prepare NASA Form 1617, Request for Cannibalization/Modification of Controlled Equipment per NPR 4200.2, Equipment Management Manual for Property Custodians, paragraph 2.3, prior to removing the storage device. For instructions on cannibalizing equipment see NPR 4200.2 and page 2 of NF 1617.



Note 4
An acknowledgment that all data and software have been removed and all memory locations have been overwritten must be prepared, signed by the System Administrator, concurred by the Line Manager, and attached to the equipment or it will not be picked up. The Line Manager has the option to witness the removal/erasure of government data.

Equipment received by the Property Disposal Officer without this acknowledgment and all required signatures will be returned.